View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Calhoun, Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Center for Information Systems Security Studies and Research (CISR) Faculty and Researcher Publications

2011-03

Center for Information Systems Security Studies and Research (CISR) Projects / MYSEA / March 2011

Naval Postgraduate School, Monterey, CA.

http://www.nps.edu/library

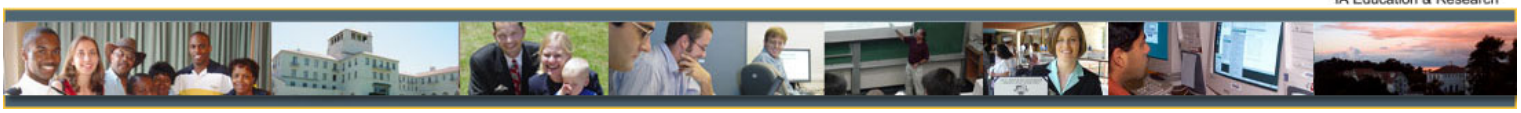
Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

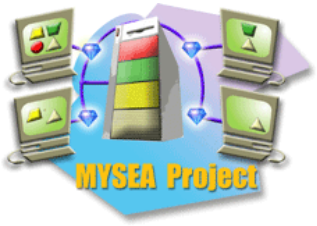
Search Site

Centers of Academic Excellence
IA Education & Research



Research: Projects: MYSEA

Monterey Security Architecture (MYSEA)



Description

The purpose of this research project is to develop high assurance security services and integrated operating system mechanisms that will protect distributed multi-domain computing environments from malicious code and other attacks. These security services and mechanisms will extend and interoperate with existing applications and open source operating systems, providing new capabilities for composing secure distributed systems using commercial off-the-shelf (COTS) components. The latter objective results from the realization that unless a secure system offers users the same sort of convenient interfaces they use when handling routine information, the secure system will fail due to lack of user acceptability.

Motivation

The necessity to protect sensitive data from day-to-day information sharing is a common predicament all through society; corporations must maintain tight control of secrets just as the military must guard its knowledge from opposing forces. Offering sensitive data protection within an everyday communications system that proves acceptable to the common user is the real dilemma. Our goals are to demonstrate the ability to enforce multi-domain access controls in existing open operating systems and to demonstrate trusted interoperability for these capabilities with open source and COTS workstations, and office productivity applications.

Approach

The MYSEA (pronounced my-see-ah) project has constructed a prototype demonstration of a potential high assurance distributed operating environment for enforcing multi-domain security policies, composed of a combination of many low-assurance commercial components and relatively few specialized (e.g., high assurance) multi-domain components. The MYSEA server is based upon the BAE Systems STOP operating system (presently EAL level 5) while the network itself supports unmodified COTS productivity applications. The demonstration architecture permits the on-going DoD and U.S. Government investment in commodity PC operating systems and applications to be integrated into a high assurance environment where enforcement of critical security policies is assigned to more trusted elements. The modularity of the architecture permits alternate configurations, for example to include an EAL level 7-evaluated high assurance multi-domain enforcement component (not yet completed) called the trusted path extension (TPE). This is a separate project titled Trusted Computing Exemplar (TCX).

For this project, we intend to demonstrate techniques for vertical integration of application security requirements with underlying security services. We have chosen the BAE Systems STOP operating system in conjunction with an internally developed software module called the secure session server (SSS). The SSS is intended to establish and maintain a point-to-point, impenetrable connection to the TPE. This design permits the client workstations to be COTS. In addition, we have included an existing Quality of Security Service model and framework called the Dynamic Security Services (DSS) into the MYSEA Testbed. This allows us to better understand the overall effects on security policy, security service, and security mechanism interactions within a network. Additionally, the MYSEA system will support single sign-on for interaction with multiple trusted servers.

Impact

We expect that this project will result in significant new and improved security functionality for existing network systems and will provide the capability to significantly reduce vulnerabilities in mission critical information systems and networks.

Status

The MYSEA project has successfully produced an operational prototype of a network with high assurance security services and integrated operating system mechanisms protecting a distributed multi-domain computing environment. Present efforts are underway to enhance the SSS module in order to improve overall efficiency and performance. As the TCX project advances future efforts will modify the TPE to the intended goal of an EAL level 7-evalutaed high assurance component.

In addition, we plan for concrete results in the following fundamental areas:

1. User access via unmodified commercial OS and applications

Users on commercial workstations will be able to access multi-domain information managed by the remote trusted OS, without modification of workstation operating systems or applications.

2. Transparent session-level access to multiple domains

Users can access data at and below their session level, providing simultaneous access to multiple data domains, as authorized by policy. This feature is provided by policy-aware protocol servers. A significant feature of our approach is that protocol servers for popular application protocols can be added to the system with only the minimal modification required for a typical platform port or can be made policy-aware with minimal additional effort.

3. Trusted path for multi-domain operating system

User authentication and session security attribute negotiation with the enhanced multi-domain OS occurs by way of a trusted path between the user and the trusted OS. Users are assured that the authentication and negotiations are with the trusted OS and not with masquerading malicious software executing on the trusted OS.

4. Remote trusted path access to multi-domain operating system

User authentication and session security attribute negotiation with the multi-domain OS occurs by way of a trusted path between the user and the trusted OS extension, as well as between the trusted OS extension and the trusted OS. Users are assured that the authentication and negotiations are with the trusted OS and

not with masquerading malicious software executing in other systems on the network, on the workstation, or the trusted OS.

5. Policy-driven dynamic network security services
Policy changes at the middleware or application level, for example as the result of changes in network situational mode or Quality of Service considerations, are automatically manifested in network connectivity maps and communication security settings (e.g., IPsec) managed with in the trusted OS.

6. Single sign-on to access multiple trusted servers
From a single session, the user can access multiple application servers on different trusted OSs, without needing to reauthenticate to each of the OSs.

Publications

C. E. Irvine, T. D. Nguyen, D. J. Shifflett, T. E. Levin, J. Khosalim, C. Prince, P. C. Clark, and M. Gondree, "MYSEA: The Monterey Security Architecture," in proc. Workshop on Scalable Trusted Computing (ACM STC), Conference on Computer and Communications Security (CCS), Association for Computing Machinery (ACM), 2009 (PDF)

Nguyen, T. D., Levin, T. E., Irvine, C. E., "MYSEA Testbed", Proceedings from the 6th IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2005, pp. 438-439. (PDF)

Irvine, C. E., Levin, T. E., Nguyen, T. D., Shifflett, D. J., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D., and Sears, J., "Overview of a High Assurance Architecture for Distributed Multilevel Security", Proceedings of the 2004 IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004. (PDF)

Irvine, C. E., Shifflett, D. J., Clark, P. C., Levin, T. E., and Dinolt, G. W., "MYSEA Technology Demonstration", DARPA DISCEX Conference, April 2003 (PDF)

Irvine, C. E., Shifflett, D. J., Clark, P. C., Levin, T. E., Dinolt, G. W., "Monterey Security Enhanced Architecture Project", DARPA DISCEX Conference, April 2003 (PDF)

Technical Reports

Clark, P.C., Wong, A., Khosalim, J., "Re-Mastering Knoppix for the MYSEA Testbed", NPS-CS-06-006, Naval Postgraduate School, Monterey, California, January 2006. (PDF)

Irvine C. E., Nguyen T. D., and Levin, T. E., "High Assurance Testbed for Multilevel Interoperability", NPS-CS-05-002, Naval Postgraduate School, October 2004 (PDF)

Irvine, C. E., Shifflett, D. J., Clark, P. C., Levin, T. E., and Dinolt, G. W., "MYSEA Security Architecture", NPS-CS-02-006, Naval Postgraduate School, May 2002 (PDF)

Theses

Egan, Melissa, /An Implementation of Remote Application Support in a Multilevel Environment, /Masters Thesis, Naval Postgraduate School, March 2006.

Bui, S., "Single Sign-On Solution For MYSEA Services", Masters Thesis, Naval Postgraduate School, September 2005 (Abstract, PDF)

Tse, L., "Feasibility Study Of VOIP Integration Into The Mysea Environment", Masters Thesis, Naval Postgraduate School, September 2005

Horn, J. F., "IPSec-Based Dynamic Security Services for the MYSEA Environment", Masters Thesis, Naval Postgraduate School, June 2005 (Abstract, PDF)

Cooper, R.C., "Remote Application Support in a Multi-Level Environment", Masters Thesis, Naval Postgraduate School, March 2005 (Abstract, PDF)

Herbig, C. F., "Use of OpenSSH Support for Remote Login to a Multilevel Secure System", Masters Thesis, Naval Postgraduate School, December 2004 (Abstract, PDF)

Sears, J. D., "Simultaneous Connection Management and Protection in a Multilevel Security Environment", Masters Thesis, Naval Postgraduate School, September 2004 (Abstract, PDF)

Downloads

MYSEA Quad Chart
2007 MYSEA Poster as (PDF) or (PPT)

People

Faculty and Staff:
Cynthia Irvine
Tim Levin
Thuy Nguyen
Paul Clark
David Shifflett
Jean Khosalim
John Clark
Phil Hopfner
Charles Prince

Students: Melissa Egan.

Sponsors

DARPA, NSA, NRO, and ONR.

Related Projects

HASP - The High Assurance Security Program

HARD - The High Assurance Remote Authentication Device Project
TCX - The Trusted Computing Exemplar Project
ISAKMPD Monitor
QoSS - Quality of Security Service Project

Key Words
high assurance security services, distributed multi-domain computing environment, secure distributed systems, multi-domain access controls, multi-domain security policies, EAL level 7-evaluated high assurance, trusted path, policy-driven dynamic network security services.

This U.S. Government Web Site is provided by the Naval Postgraduate School's Center for Information Systems Security Studies and Research for official information regarding CISR's programs and research.